**CHAPTER ONE**

**INTRODUCTION**

**1.1 Background to the Study**

In an increasingly digital world, the proliferation of counterfeit certificates and fraudulent claims of credentials has become a significant challenge for educational institutions, employers, and certification bodies. As technological advancements continue to evolve, it is imperative to leverage innovative solutions to combat this growing concern. One such solution is the implementation of a QR Code-Based Certificate Authentication System, a secure and efficient mechanism that ensures the validity and authenticity of certificates issued by institutions.

The traditional methods of verifying certificates often involve tedious, manual processes that are time-consuming, error-prone, and susceptible to manipulation (Chen et al., 2023). This has resulted in a demand for more robust and automated systems capable of addressing these limitations. The use of QR codes, combined with modern encryption technologies, offers a scalable and cost-effective way to authenticate certificates. QR codes, as two-dimensional barcodes, can store vast amounts of data in a compact and easily accessible format, making them an ideal tool for certificate verification.

The increasing adoption of smartphones and internet connectivity globally has made QR codes a preferred technology in various domains, including education, healthcare, and commerce (Wang & Li, 2023). With a simple scan, a QR code can provide instant access to certificate details, ensuring that stakeholders can verify the authenticity of the document in real-time. This approach not only reduces the risk of forgery but also enhances trust and transparency in the certification process (UNESCO, 2021).

Recent studies have highlighted the growing concerns surrounding fraudulent certificates. According to Smith et al. (2022), educational institutions face reputational damage and financial losses due to the circulation of counterfeit certificates. Employers, too, are at risk of hiring unqualified individuals based on falsified credentials. These issues underscore the need for a secure, automated system that can mitigate such risks and streamline the verification process.

The QR Code-Based Certificate Authentication System addresses these challenges by leveraging cutting-edge technologies to create a secure and efficient platform for certificate issuance and verification. The system utilizes QR codes embedded with encrypted data linked to a centralized database, ensuring that only authorized personnel can access and verify certificate details. By adopting this innovative approach, educational institutions and organizations can safeguard their credentials and maintain the integrity of their certification processes.

**1.2 Problem Statement**

The traditional approach to certificate authentication poses several challenges, including inefficiency, high costs, and vulnerability to fraud. Verifying the authenticity of certificates often involves lengthy manual processes, which are not only time-consuming but also prone to human error (Lee & Park, 2023). This outdated system fails to keep pace with the increasing demand for secure and instantaneous verification methods in today's fast-paced digital environment.

Research by Johnson (2023) highlights the growing prevalence of counterfeit certificates, which undermine the credibility of educational institutions and certification bodies. Fraudsters can easily replicate traditional certificates using modern printing technologies, making it difficult to distinguish between genuine and fake credentials. Employers and institutions often lack the tools to verify certificates quickly and accurately, resulting in significant challenges during recruitment and admissions processes.

Furthermore, the lack of a centralized, accessible database for certificate verification exacerbates these issues. Williams (2023) pointed out that existing systems are often fragmented, making it difficult for stakeholders to obtain reliable verification information. This fragmentation not only delays the verification process but also increases the risk of fraudulent activities.

From the above, it is evident that the current methods of certificate authentication are inadequate in addressing the challenges posed by counterfeit credentials. There is a pressing need for a more secure, efficient, and scalable solution to ensure the integrity of certificates and protect the interests of educational institutions, employers, and other stakeholders.

**1.3 Aim and Objectives**

The aim of this project is to pprovide asecured QR Code-Based Certificate Authentication System to enhance the security and efficiency of certificate verification processes. The specific objectives include:

1. To model a system that generates and embeds unique QR codes on certificates issued by educational institutions.
2. To implement a user-friendly interface for stakeholders to verify certificate authenticity by scanning QR codes.
3. To develop a secure database system for storing and managing certificate information linked to QR codes.

**1.4 Significance of the Study**

The successful implementation of a QR Code-Based Certificate Authentication System will have far-reaching benefits for educational institutions, employers, students, and other stakeholders:

The system will enhance the credibility and reputation of institutions by ensuring the authenticity of certificates issued. Automation of the verification process will reduce administrative burdens and improve operational efficiency. Institutions will be better equipped to combat certificate forgery and maintain the integrity of their credentials.

Employers will gain access to a reliable and efficient tool for verifying the qualifications of job applicants, reducing the risk of hiring unqualified individuals. The system will save time and resources spent on manual verification processes.

Certificate holders will benefit from increased trust in their credentials, enhancing their employability and academic opportunities. The QR code-based system will provide a convenient way for individuals to showcase their certificates and prove their authenticity.

The project will serve as a valuable reference for further studies on the application of technology in document authentication and security. Insights from the system's implementation can inform the development of policies and standards for digital certificate verification.

* 1. **Scope of the Study**

This project focuses on the design and implementation of a QR Code-Based Certificate Authentication System for educational institutions. The system will include the following features: Integration of QR codes on certificates issued to students, containing encrypted data linked to a centralized database, A web-based platform accessible to stakeholders for scanning QR codes and verifying certificate details, a secure database for storing certificate information, ensuring data integrity and protection against unauthorized access, role-based access control for administrators, students, and verifiers to ensure system security and Implementation of encryption and authentication mechanisms to prevent data tampering and ensure the privacy of certificate information.

**1.6 Definition of Operational Terms**

**Authentication**: The process of verifying the validity and authenticity of a document or credential.

**Certificate**: An official document issued by an educational institution or organization to certify an individual's achievements or qualifications.

**Database**: A structured collection of data stored electronically and managed using software systems.

**Encryption**: A security technique used to protect data by converting it into an unreadable format, accessible only to authorized parties.

**QR Code**: A two-dimensional barcode that stores data in a compact and easily scannable format.

**Verification**: The process of confirming the authenticity and validity of a certificate using predefined methods or tools.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 Overview

This chapter consist of previous project work carried out as related to the project, it sets the theoretical framework or base for the project and it also gives a brief explanation of the various terms pertaining to the research project.

## 2.2 Quick Response Code

QR (Quick Response) codes have gained significant popularity in recent years due to their versatility and ease of use. They are two-dimensional barcodes that can store a large amount of information, including text, URLs, contact details, and other data, in a compact format. QR codes consist of black modules arranged on a white background, forming a square or rectangular shape. These codes can be scanned and decoded using mobile devices with camera functionality and QR code scanning applications (Wachirawutthichai *et al.,* 2022).

QR codes offer several advantages that make them suitable for various applications. They are easily readable by smartphones and can be scanned quickly, providing a seamless user experience. The error correction capabilities of QR codes allow for accurate decoding even if the code is partially damaged or distorted. Additionally, QR codes can store more information compared to traditional barcodes, making them ideal for storing complex data structures or URLs. Researchers and practitioners have explored the applications of QR codes in diverse fields. For instance, in marketing, QR codes are utilized to provide quick access to product information, promotions, or loyalty programs. They are also employed in ticketing systems, allowing users to easily access electronic tickets for events, transportation, or attractions. Furthermore, QR codes have found use in document verification, enabling the authentication and validation of various certificates, licenses, and identification documents (Yang et al., 2023).

Recent studies have focused on enhancing QR code technology to address specific requirements and challenges. For example, researchers have proposed techniques to improve the security of QR codes, such as incorporating encryption mechanisms to protect sensitive information encoded within the codes (Hsu et al., 2022). Other studies have investigated methods to enhance the visual aesthetics of QR codes by incorporating design elements or patterns while preserving their scannability (Tang et al., 2021).

## 2.3 Document verification

Document verification is a vast field such that there is bank type of documents, governmental type of documents, transactions type of document, educational certificates type of document and many more other kinds. Each of the domain and types can be treated differently and the content vary tremendously. For example, transactions can contain number in tabular form while educational certification may contain only textual information presented in paragraphs. Due to the vast differences in types of documents and how they are presented the research will focus on digital verification of paper-based graduation certificates.

Verification is the process of determining or confirming that someone (or something) is original. Documents Verification on the other hands can be define in various ways such as the researchers Warasart and Kuacharoen, (2012), defines document verification as the process of proving the correctness or authenticity of a document by using a proven method or technique. While the researchers Osman and Omar (2016), defines it as the process of ensuring that documents received from holder are genuine and that the holder is the rightful owner. Verification is the evidence that establishes or confirms the accuracy or truth of something while verifying is the act to prove the truth of, as by evidence or testimony.

A certificate verification is the act to prove that a certificate rightly and legally belongs to an organization or an individual or both. It is a computerized means of verifying someone’s claim of certificate- ship from an institution. Online Certificate Verification system improves the speed, quality of service of certificate authentication, globalization of markets, and cuts down cost (Nwachukwu & Igbajar, 2015). Educational establishments try to combat fraud and forgery in several ways, however, most of the methods are time-consuming because they are manual, partly automated or involve human to human interaction (Osman & Omar, 2016).

The main aim of document verification is the ability to trace the origins of a document to a specific person, the device that produced it or the place where it was produced (Srushti, Sanket, Aman, and Tyagraj, 2014). Forgeries pose a huge threat to the integrity of documents, with significant dangers in terms of authentication and trust. It is therefore important to protect the integrity of a document in order to prevent problems arising from the modification of a document by intruders (Srushti, Sanket, Aman, and Tyagraj, 2014). According to the research conducted by Nwachukwu and Igbajar (2015), all documents or credentials that are printed are potentially subject to counterfeiting and forgery. Forgery can cause a lot of damage when it comes to trust and authenticity (Hampo, 2011).

There is a high market for forgery as well as opportunity with low cost, high quality results available (Warasart, & Kuacharoen, 2012). Researchers have also found several significant problem areas when it comes to document verification. For instance, the technologies that are put forth to stop or prevent forgery do not seem to be moving as fast as the evolution of the forging techniques (Singhal, & Pavithr, 2015). With respect to academic documents, further authentication problems include the variations from one school to the next, which causes consistency issues that can be taken advantage of, especially in international situations (Boukar, Yusuf & Muslu, 2017).

There are two basic document categories that are considered in document verification literature; digital based documents and the traditional paper or printed document. The research in this case deals with certificates. Almost all documents can be handled in a digital manner, except for the certificate. The reason for this exception is that all digital documents are easy to forge without leaving any clues (Tint & Win, 2014). Furthermore, the prevalence of forged certificates results from the increased global demand for higher education, which exceeds the university capacity of the world (Boukar, Yusuf & Muslu, 2017).

According to the research conducted by Tint and Win (2014), there are two main types of forgery, type 1 and type 2. Type 1 forgery is when some part of the original document is changed in order to benefit someone who was not benefitted by the original document. In this case, the base substance, normally the paper or plastic card, remains legal and valid, but the information that is contained therein is forged. The second, type 2 forgery is when both the base substance and the information contained therein is fake. However, it is often very difficult to tell whether it is real or fake because the base substance and the style of the document normally look authentic (Tint & Win, 2014). The researchers of the research Tint and Win (2014), outlined the characteristics of the classic unforgeable document. They also outlined three principles of the unforgeable document as follows;

1. The forged document normally has some difference from an authentic original document in some way
2. The detection of the forgery can happen without reference to the authentic original document
3. There is a concrete verification method that does not necessarily involve communication with an authentication bureau

## 2.3.1 Types of documents

Documents can be categorized to two categories which are paper based documents and digital based document (Tint & Win, 2014). Paper based document contains characters, digits, tables, etc. Its digital version or digital document is a computer file. Digital document is designed to produce visual information on the computer monitor (Tint & Win, 2014). Forgery of documents has increased jeopardizing the integrity of both the document holder and the organization that issued the document. The forgery of document is classified into two types which are 1) altering part of an authentic document that is original and 2) producing a new fake certificate with false information (Tint & Win, 2014). Forgery of document has become easier than the past mainly because of the technological advancements. For example, scanning and printing hardware are much more advanced than they use to and are not as expensive add to that the editing software that are widely spread and constantly being updated and enhanced. Unfortunately, as document forgery has become easier the increase of fake document has also increased. The latter is due to the lack in advancements in securing as well as verifying the paper-based documents (Osman & Omar, 2016). In other words, documents securing and verification are not advancing as fast as the tools that enable forgery are. For that, the document verification became an important task; it is the process of ensuring that documents presented by prospective employees are genuine and that the holder is the rightful owner.

## 2.3.2 Paper based document

This section will describe and detail on the first type of documents mentioned earlier and is the paper-based documents. Its importance is described and also how they are verified.

The paper-based documents are still widely used. There are many types of paper-based document such as graduation certificates, birth certificates, etc. The information inside the paper-based documents are subject to threats like forgery; despite measures taken to protect them attacks still happen. Authors Boukar, Yusuf and Muslu (2017), attributes that to the lack of verification. There are many cases where documents where forged throughout the globe. For example, one that happened in New Delhi, where five people obtained loans and cheated the banks using fake documents (Osman & Omar, 2016). Another example is one that happened in Bagdad, an investigation of 20,000 government employees by Iraqi's parliament showed that some employees have used forged educational certificates and fake diplomas to get their jobs. The issue extended in that those employees that used fake certificates became senior officials in the government (Srushti, Sanket, Aman, and Tyagraj, 2014). Forgery of documents can happen in any discipline or line of work. In U.S. for example, The National Health Care AntiFraud Association projected that United States of America lost 3% to 10% of total healthcare cost to fraud (GeeksforGeeks, 2018). Another example of forgery that happened in an area that involved the medical discipline is in Malaysia. The mainstream newspaper reported that a statement given by the Congress of Unions of Employees in the Public and Civil Services (CUEPACS) stated that more than 45,000 or 3% of 1.5 million government’s staff in Malaysia forged medical certificate as a reason of absence from work to do part-time jobs. Another discipline that was impacted is Education.

With that has been mentioned document verification is important to overcome many issues that could even do with life and death. Imagine a doctor forging his way into a medical school. Or a politician forging his way to power. As a result, many could be harmed of such a behavior. Document verification of a paper-based document has to be efficient to allow of seamless verification.

## 2.4 Certificate Verification Systems

Certificate verification systems play a crucial role in ensuring the authenticity and integrity of certificates in various domains such as education, healthcare, finance, and legal documentation. Recent studies have focused on developing efficient and secure certificate verification systems, incorporating innovative approaches and technologies. This section presents a review of recent research in this area, highlighting methodologies, advantages, and limitations of certificate verification systems. Researchers have proposed different approaches to certificate verification, aiming to enhance the overall security and reliability of the process. Some studies focus on QR code-based verification systems, leveraging the unique capabilities of QR codes to embed encrypted information and facilitate efficient scanning and decoding. For instance, Hu et al. (2021) proposed a lightweight certificate verification system using QR codes for e-commerce, providing a secure and efficient method for verifying product certificates and authenticity. This system utilized QR codes to store encrypted product information and integrated it with a verification algorithm to ensure reliable validation.

In addition to QR codes, other technologies have been explored to enhance the security of certificate verification systems. Blockchain technology has gained significant attention due to its decentralized and immutable nature. Researchers have proposed integrating blockchain with certificate verification systems to establish a tamper-proof and transparent verification process. Kshetri and Voas (2022) presented a trustworthy certificate verification system using QR codes for Internet of Things (IoT) devices, combining QR codes and blockchain to verify the authenticity and integrity of IoT device certificates. The utilization of blockchain technology provides a decentralized and auditable system for certificate verification.

Furthermore, studies have investigated the integration of additional security measures into certificate verification systems. Wang and Li (2023) designed and implemented a certificate verification system using QR codes in higher education, incorporating steganography to enhance the security of embedded information within QR codes. Steganography allows the hiding of information within images, thereby providing an extra layer of security to the certificate verification process.

Advancements in machine learning and artificial intelligence (AI) have also been leveraged to improve the accuracy and efficiency of certificate verification systems. Researchers have explored the use of machine learning algorithms to automate the verification process and detect fraudulent certificates. For example, Li et al. (2021) proposed a machine learning-based certificate verification system that utilizes image recognition techniques to analyze and verify the authenticity of certificates.

While certificate verification systems have shown significant advancements, they also face certain limitations and challenges. One of the key challenges is the management of a large volume of certificates and verification requests. Ensuring scalability and efficient data storage and retrieval mechanisms are crucial in maintaining the performance of the system. Interoperability with existing systems and user acceptance are also important factors to consider in the design and implementation of certificate verification systems.

## 2.5 Graduation certificate

A university is an example of an organization that creates so many documents for their students. It issues a certificate and academic transcript for each of its graduates. The certificate contains information that certifies a person has graduated from a certain specialization and obtained results as stipulated in the certificate. The certificate can then be used for job hunting or pursuing academics or any other purpose. The graduation certificate issued by the universities/institutions is one of the important documents for the graduate. It is a proof of graduate’s qualification and can be used anywhere. Every year millions of students graduate from colleges and Universities, and their numbers are growing. Institutions issue certificates to those who have successfully completed the requirements of graduation. A graduation certificate is still in the form of a paper-based document because, as of yet, an electronic document cannot effectively replace a physical certificate (Smartsheet, 2019). With the rise of graduates and advancements in printing and photocopying technologies, came the rise of fake certificates as well threatening the integrity of both the certificate holder and the university that has issued the certificate (Abolaji, 2017).

The graduation certificate has to be verified to ensure that its content is true and also to ensure that the issued certificate comes from a real source (Osman and Omar, 2016). Fake certificates can be created easily and the quality of a fake certificate can now be as good as the original. The certificates of many prominent universities have been forged and these forgeries are very difficult to detect. Educational establishments try to combat fraud and forgery in several ways Hampo (2011); however, most of the methods are time consuming because they are manual and involve human interaction. A lot of the time is spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university that the certificate is valid and true. This process can be extremely laborious and expensive especially if a company needs to check the certificates of several hundreds of applicants. This adds to need of having a cost-effective fast solution to verify certificates.

## 2.5.1 Importance of Graduate Certificate

Graduate certificates are of great importance to land a job or pursue further education they are the proof that the holder possesses the necessary knowledge to take a given position or pursue education. If these certificates are forged the whole foundation could collapse such that the employee would hold a position is not entitled to and could ruin or bring down the company. If it is in an educational institution, it could mean many things of which a seat could be occupied by unworthy person instead of a worthy person.

## 2.5.2 Paper-Based Certificate

Paper based certificates are still widely spread mostly because it is considered more secure than the digital certificate (Srushti, Sanket, Aman, and Tyagraj, 2014), (Singhal an&d Pavithr. 2015). Paper based certificate have stamps and signatures on them which can reflect originality (Abolaji, 2017). Many entities require a stamp and a signature to accept a given document and graduation certificates are no different. However, the issue that arises is that the holder would be bound to providing the original copy every time the stamp and signatures are required. Another importance for paper-based certificate is that they are easy to note from and on; Say the manuscript; modules can easily be highlighted and marked. Allowing multiple reviewers to go through it and do the same.

Paper based certificates despite being widely used they can be damaging. The most important disadvantages are:

1. With paper-based certificates is risk of loss and damage. Paper based certificates can easily be lost especially now as it is easy to relocate between different places and countries.
2. Paper-based certificates is that they can be costly especially if changes are required on the document; for example, a faulty name was printed, more papers would have to be used and that extra cost for the entity issuing the certificate; this indirectly also effects the environment.
3. Paper based certificates can easily be damaged be it a wet hand or a fire in the building; Once the paper documents are damaged, they are usually hard to recover. The holder either has to travel to source to generate the same or if the same is not regenerated it is a loss.
4. Paper based certificates can eventually consume physical space.
5. Paper based certificates can be slow to retrieve.

Despite these drawbacks with Paper based certificates entities still use it.

## 2.5.3 Digital based Certificate

The graduate digital certificate is the certificate that is issued in a digital form. It usually issued through a secure certification and verification method (Tint & Win, 2014). It is mostly adopted in order to solve the management problems of paper-based certificate. However, one of the important reasons why digital certificates are widely adopted is that digital certificates provide a unique feature which is portability (Adams & Blandford, 2012); it is easy to transfer documents when they are digital.

Digital based certificates are considered environment friendly and can easily be organized without taking much space. The digital certificates in the simplest form is the easiest to forge without the need for special hardware (Adams & Blandford, 2012). Editing softwares are widely spread and changes to manuscripts and graduation certificates can easily be made. Digital certificates are easily generated and can be amended with ease. Despite the advantages the digital based certificates they are not widely spread as the paper-based certificates and are not the preferred method for many universities. Even if digital based certificates are issued paper-based certificates are still required and needed.

## 2.6 Models for a Certificate Verification System

Web-based applications are fundamental to modern digital interactions, and their architecture significantly impacts their performance, scalability, and reliability. The choice of architecture model depends on the complexity of the application and its anticipated traffic and usage. Let's delve deeper into the three primary models of web application components with insights from recent literature.

## 2.6.1 One Web Server with One Database

The simplest model, involving a single web server and a single database, is often used for small-scale applications or during the initial development and testing phases. This model is straightforward and easy to manage but poses significant risks in terms of reliability and scalability. If the single server experiences downtime or failure, the entire application becomes unavailable, which can be detrimental for production environments (Srinivasan, 2020). According to a study by Zhang *et al.* (2021), this model is particularly useful for prototyping and early-stage startups where the primary goal is to validate the idea rather than ensuring high availability.

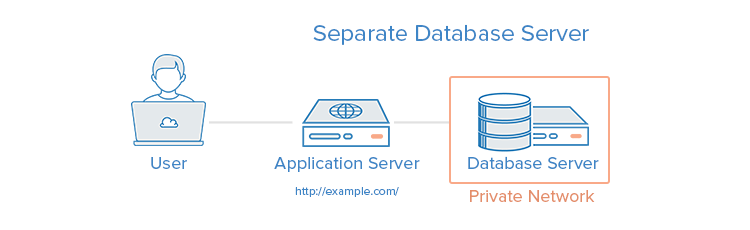


Figure 2.1: One Web Server with One Database

Liu *et al.* (2022), explored the design and implementation of a secure and scalable e-commerce platform using a single web server with one database. The research focused on optimizing server performance and database queries to handle increasing loads while maintaining security. The results demonstrated that with proper indexing and query optimization, a single server architecture can effectively serve a moderate-sized e-commerce site, though scalability issues may arise as traffic grows.

In another study by Smith *et al.* (2023), the performance optimization techniques for small-scale web applications using a single web server with one database were investigated. The study emphasized the importance of efficient database indexing, query optimization, and caching strategies. The results indicated that even small web applications could achieve significant performance improvements and better user experience through these optimization techniques.

## 2.6.2 Multiple Web Servers with One Database (Stateless Architecture)

The model of multiple web servers with one database, also known as stateless architecture, is an intermediate solution that balances simplicity and reliability. This approach involves deploying multiple web servers that do not retain any user session information, relying instead on a centralized database to manage all data and state information. The stateless architecture with multiple web servers and a single database offers a balance between simplicity and reliability. In this model, the web servers do not store session information; instead, they rely on the database to handle state persistence (Li *et al*., 2021).

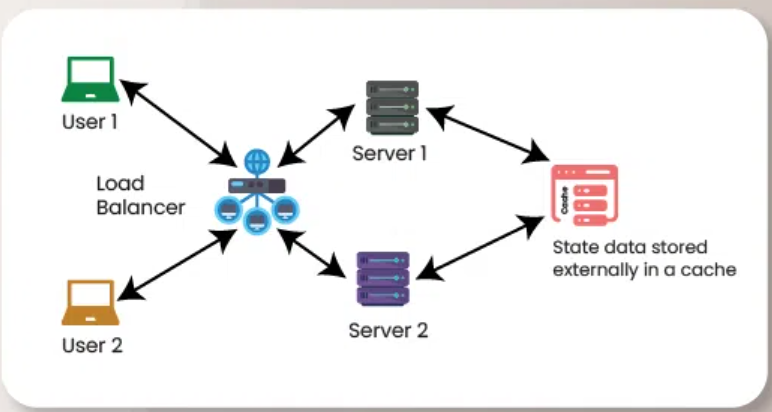


Figure 2.2: Stateless Architecture

Kumar *et al.* (2023), a stateless architecture with multiple web servers connected to a single database was implemented to enhance load balancing and redundancy in a high-traffic web application. The research found that this approach significantly improved system reliability and performance under heavy load by distributing requests across multiple servers, thus preventing any single server from becoming a bottleneck.

Jones *et al.* (2022), explored the use of a stateless architecture with multiple web servers connected to a single database for e-learning platforms. The research focused on enhancing scalability and reliability to handle peak usage during online exams and lectures. The findings demonstrated that this architecture could effectively distribute the load and improve system availability, ensuring a seamless learning experience for users.

## 2.6.3 Multiple Web Servers with Multiple Databases

The architecture of multiple web servers with multiple databases represents the pinnacle of web application design, offering high availability, fault tolerance, and scalability. This model is complex but essential for applications with significant traffic and data demands. One of the primary advantages of this architecture is its high availability. By distributing data across multiple databases and deploying multiple web servers, the system can withstand failures without significant downtime. If one server or database fails, others can seamlessly take over, ensuring continuous service availability. According to Karger *et al.* (2021), this redundancy is critical for applications requiring near-zero downtime, such as financial services and e-commerce platforms.

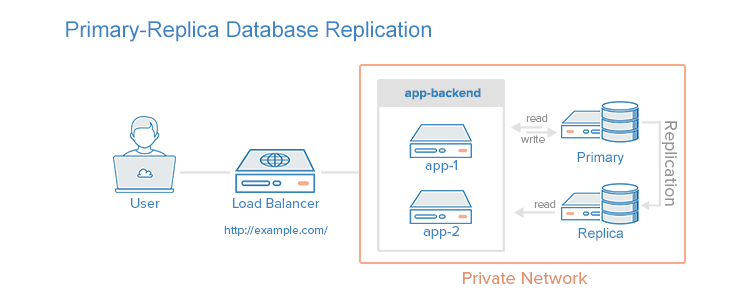


Figure 2.3: Multiple Web Servers with Multiple Databases

Chen *et al.* (2023), conducted a study on using multiple web servers with multiple databases to manage a large-scale web application. The research focused on database sharding and replication strategies to ensure data consistency and availability. The results showed that this architecture significantly improved the system's ability to scale horizontally and handle high volumes of transactions while maintaining data integrity.

Martinez *et al.* (2023), examined the implementation of high-availability web services using multiple web servers with multiple databases. The research highlighted the use of database replication and failover mechanisms to ensure continuous service availability. The study concluded that this architecture significantly enhances fault tolerance and minimizes downtime during database failures.

## 2.6.4 Microservices Architecture model

Microservices architecture breaks down applications into smaller, independent services that communicate through APIs. Each service is responsible for a specific business function and can be developed, deployed, and scaled independently. This approach contrasts with monolithic architectures where all functionality is bundled into a single application.

Microservices allow each service to be scaled independently based on demand. This granular scalability is advantageous for applications with varying traffic patterns or specific service-level requirements (Newman, 2015).



Figure 2.4: Microservices Architecture model

In a 2022 study by Rodriguez *et al*., the implementation of a microservices architecture was examined in the context of agile software development. The research demonstrated that microservices allow for independent deployment and scaling of services, which enhances development speed and system resilience. The study also highlighted the benefits of using containerization and orchestration tools like Docker and Kubernetes.

Nguyen *et al.* (2022), conducted a study on the adoption of microservices architecture in financial technology (fintech) applications. The research focused on the benefits of microservices in terms of scalability, flexibility, and rapid deployment. The study found that microservices enabled fintech companies to quickly adapt to market changes and regulatory requirements while maintaining high levels of security and performance.

## 2.6.5 Serverless Architecture model

Serverless architecture, also known as Function-as-a-Service (FaaS), abstracts server management and infrastructure concerns from the developer. In this model, developers write and deploy individual functions that are triggered by events, such as HTTP requests or database updates. The cloud provider manages the underlying infrastructure, automatically scaling resources as needed.

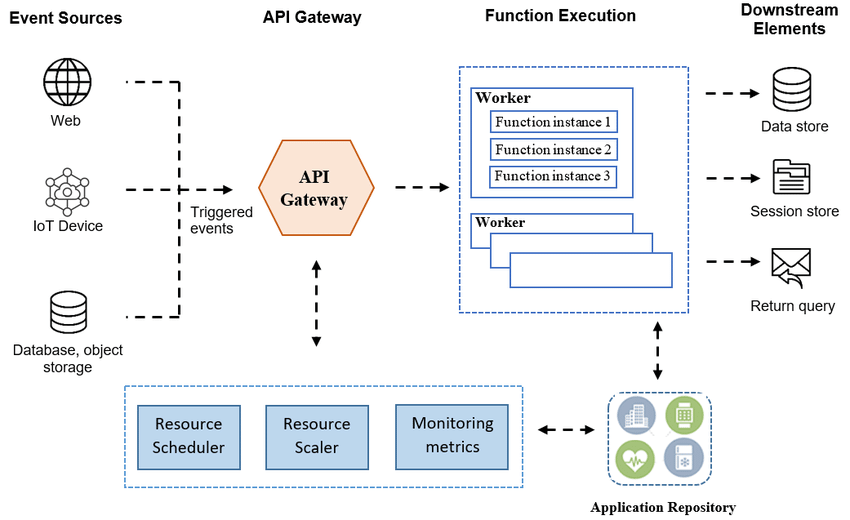


Figure 2.5: Serverless Architecture model

In a study by Patel *et al.* (2023), the use of serverless architecture in cloud resource management was explored. The research found that serverless computing allows developers to focus on code without managing underlying infrastructure, leading to significant cost savings and increased agility. The study also, discussed the challenges of cold starts and the importance of optimizing function execution times.

Adams *et al.* (2023), the use of serverless architectures for real-time data processing was examined. The research demonstrated that serverless computing could handle large volumes of real-time data efficiently, with automatic scaling and reduced operational costs. The study also addressed challenges related to latency and the need for optimizing serverless functions for quick execution.

## 2.7 Review of related literatures

Since (1995), or what Tenopir calls the “post web world” (2003), libraries have been seen as in danger of “substitution” The web is becoming “a ubiquitous source of information” giving an “illusion of depth and comprehensiveness” that leads to a questioning of the value of libraries and their collections. This review will not speculate on these future roles, but will focus instead on the certainty of changing technology, increasingly digital information resources and societal shifts that have changed user expectations of online certificate verification system.

Several approaches have been made to verify certificates and clear the issue of certificate forgery, however, certificate verification method still prevalent today is a manual process, whereby, whoever wants to verify a certificate trips to the institution or send a written request.

In light of the above, Srushti et al. (2014) presented a certificate generation system to ensure an efficient certificate management using huge data and to provide mark sheets for credit-based grading system (CBGS) in a very user-friendly manner. In this system, the admin enters the marks of each student. That information will be stored in internal collection information database, percentage and grade is calculated manually. The system embedded the digital form in mark sheet using encrypted QR code, so that any unauthorized user cannot retrieve any information. However, the system is partly automated made it inefficient.

Hampo (2014), in his work adopted the Structured System Analysis and Design Methodology (SSADM) which emphasizes on completing a phase of the software development before proceeding to the next phase and also being able to go back to the other phases in a purely sequential manner. The model used for this project is the Rapid Application Development (RAD) model proposed by International Business Machine (IBM) in 1980 and introduced to software community by James Martins through his book Rapid Application Development. Unfortunately, it was not a web-based application but a desktop application software which made the system less valuable as compared to web applications.

Osman and Omar (2016), incorporated cryptography approach and cloud-based model to enhance the verification mechanism and thereby reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved. By using the Cloud-based model, some of the factors that result in reduced operational efficiency in student services at universities can be addressed and this should have a positive impact on the quality of services provided by universities. However, since cloud infrastructures are owned and managed by service providers, the cost of implementation is also high. Thus, most institutions could not afford its implementation.

Yusuf, Boukar and Shamiluulu (2018), research work enabled an end-user to define certificate template and template format without the requisite of XML knowledge by clicking few buttons and typing from the system GUI, verifying the certificate and generating one or more certificate(s) simultaneously. In the system, students' details are imported into the system using an excel file, thus, making the system partly automated and inefficient. Singhal and Pavithr (2015), to prevent the circulation of fake degree certificates adopted the use of the QR Code and Smart Phone Application. A QR Code contains a digital signature over the data such as degree holder's name, enrollment number, roll number, total marks obtained etc. which will be signed by university authorities. To verify the digital signature a person needs to use a specific smartphone application which will scan the QR Code and authenticate the certificate. The system was able to combat certificate fraud by embedding the QR Code on the degree certificate and by introducing the smartphone application which will read the digital data from the QR Code. It enables the verification of the certificate without depending on the certificate issuing institution. This did not only improve the authenticity mechanism of a certificate at a much faster rate than manual verification but also prevents the creation of fake certificates through cost-effective.

Musee (2015), in his study Employed Agile Methodology approach and Unified Process modelling to develop a cloudbased prototype which is used as SaaS to provide certificate verification. The prototype allowed users to request to get the academic certificates verified by filling the name of institution, course name, year of graduation and the verification code. All these processes were carried out in private cloud and accessible online.

Boukar, Yusuf and Muslu (2017), adopted the use of Java DataBase Connectivity (JDBC) and MySQL connector jar file hence designed a web-based approach proposed to replace the traditional (manual) verification process by retrieving certificate data from institutions in JSON format and archiving them in a database from which verification can be made eliminating security threats and human error. An SQL query was executed to retrieve relevant information from the database. Results are parsed and presented in a JSON format using the GSON jar file and JSON library functions. However, the use of NoSQL features in MySQL became the major deficiency of their system as it slows down the system operation.

Tint and Win [10] to control fake certificates, considered the combination of Elliptic Curve Digital Signature Algorithm (ECDSA) and Secure Hash Algorithm-1 (SHA-1) algorithm which provides strong cryptographic strength and optimizes the computational speed as well as space. In this process, the input message from the user is hashed into a message digest. This digest code is encrypted into signature value using the ECDSA algorithm. The signature value is converted into barcode. The user input message and barcode are combined into electronic certificate. If a user is a new user, he/she must register first. This user needs to input his/her information and generate public/private key pair. This user information and private key will be used to create an electronic certificate. The system, however, lacked the certification authority (CA) between user and server for a trusted third-party system and to get a more secure client-server authentication system.

Warasart & Kuacharoen (2012), in their paper, implemented a paper-based document authentication in which a document can be verified with the use of a digital signature and QR code. This enables the verification of the documents without depending on any special institute such as the forensic science centre or accessing the database. The verification process can be done automatically if the Optical character recognition or optical character reader (OCR) is accurate. Otherwise, human inspection is required. The inspector can see the differences between the printed message and the message in the QR code. This semi-automated process is the major drawback of their system.

Nwachukwu & Igbajar (2015), considered the adoption of Top-Down structure (a modular approach) with Iterative model and designed an online certificate verification system that can be implemented as a standalone application or embedded in a school official website depending on how the institution decides to use it.

The system was based on an RDBMS for certificate storage though can automate the process of certificate creation and management but lacked partition tolerance i.e. horizontal scalability, Flexibility and above all Efficiency when data became very large.

## 2.8 Summary

Based on what has been presented in the previous sections, there are many techniques proposed for paper-based document verification. Most of these techniques require change in the process of certificate generation either by changing template, changing paper, changing printers, adding hardware or even adding extra information. This change may mean that the university or verifier need the proper knowledge to execute and run the proposed technique. This also mean that older certificates may not work with the new introduced techniques. To also add some proposed techniques, require a change that is not always easy or cheap like in creating a third body to verify certificates.

As reflected some techniques are mostly suitable for specific domain and document like signature extraction for bank cheques. Others were proposed based on specific environments and conditions like environments that assumes both send and receive are known to each other (Osman & Omar, 2016), (Henrieta, 2015).

# CHAPTER THREE

# METHODOLOGY

## 3.1 Overview

This chapter provides an in-depth analysis and design of the proposed Certificate Verification system, focusing on its benefits and improvements over existing verification process. It begins by evaluating the current systems—both manual and automated—highlighting their limitations such as inefficiency, outdated information, and challenges in matching tutors with students. The discussion then shifts to the proposed system, which addresses these issues with enhanced efficiency, real-time updates, advanced matching algorithms, and a user-friendly interface. The system's advantages include improved accuracy in tutor-student matches, robust data management, scalability, and flexibility, all contributing to a more effective solution for managing tutor allocations and student inquiries.

Additionally, the chapter outlines the hardware and software requirements necessary for implementing the Certificate Verification system, detailing the technical specifications for both server and user devices. It describes the system architecture and design, including the interaction between various components and the design of user interfaces. The methods of data collection used for this study are also covered, with a focus on primary sources such as interviews and questionnaires, and secondary sources like academic journals and industry reports. The chapter concludes by addressing the transition from manual processes to an automated system, outlining the implementation plan, potential challenges, and solutions to ensure a smooth and successful deployment.

The proposed Certificate Verification system also incorporates advanced search and filtering capabilities, allowing administrators to refine their search based on specific criteria such as date, department, course. This feature significantly enhances the user experience by providing tailored results that align closely with the institution needs. Furthermore, the system’s backend is designed to support real-time communication between tutors and students, enabling immediate interactions that facilitate quicker decision-making and scheduling. The integration of notifications and reminders ensures that both parties remain informed of upcoming sessions and any changes, thereby reducing the likelihood of missed appointments or misunderstandings.

Moreover, the chapter explores the security measures implemented to protect user data and ensure privacy. Given the sensitive nature of the information exchanged within the platform, such as personal details and payment information, the system employs encryption and secure authentication methods to safeguard against unauthorized access. Regular security audits and updates are planned to maintain the integrity of the system. The chapter emphasizes the importance of these security features in building user trust and ensuring compliance with relevant data protection regulations. The proposed system, therefore, not only improves the efficiency of finding and connecting with tutors but also provides a secure and reliable platform that users can confidently rely on.

## 3.2 Methods of Data Collection

This study will adopt two methods of data collection:

**Primary Source:** Primary source refers to the sources of collecting original data in which the researcher makes use of empirical approach such as personal interview, questionnaires or observation.

**Secondary Source:** The need for the secondary sources of data for this kind of project cannot be over emphasized. The secondary data were obtained from magazines, Journal, newspapers, library source and most of the information from the library research has been covered in the literature review section.

## 3.3 System Analysis

## 3.3.1 Analysis of the Existing system

Certificate verification method that is prevalent today is a manual process, in this process the institution/organization that want to verify a result will have to make a trip to the university or send a written request so as to verify result. The request will then go to academic affair which refer to the library or safe files to look for the duplicate certificate, this can really be time consuming, also sometimes files are lost when moved from one office to another, and in some cases, can be missing or be difficult to locate.

The registrar might be very busy with so many other letters and thereby read the letter late. It will take a while for the letter to be replied and sent back. The body that wants to verify a certificate can equally send a representative to the school; such trip will end up costing the body that needs to verify the certificate. The manual method of verifying the certificate is usually cost incurring, not fast, prone to error etc.

## 3.3.2 Problems of the Existing System

Such conventional methods pose several drawbacks:

1. Time-consuming processes: Manual allocation procedures, involving paperwork and face-to-face coordination, can significantly consume time. This can lead to delays in tutor allocation and scheduling.
2. Administrative burden: Managing and verifying certificates manually requires considerable administrative effort, including record-keeping, communication, and scheduling. This increases the workload for departmental staff and can lead to inefficiencies and errors.
3. Limited access to information: Manual systems may not provide easy access to comprehensive tutor profiles, leading to suboptimal matching between tutors and students based on skills and preferences.

## 3.4 Proposed System

System design for the Certificate Verification involves defining the platform's architecture, modules, interfaces, and data structures to meet specified requirements. It entails the application of systems theory to product development, ensuring the alignment of design elements with the objectives and needs of the institution.

The proposed Certificate Verification system offers numerous advantages over manual allocation methods:

1. Efficiency in generation: The online platform streamlines the process of generating certificates for students with details such as student name, registration number, quick response (QR) code, thereby reducing the time required for certificate verification.
2. Reduced administrative workload: Automated processes for certificate generation and verification and alleviate the administrative burden on departmental staff, allowing them to focus on other critical tasks.
3. Enhanced accessibility: The online platform provides easy access to certificate verifications by employers of labour based on their qualifications and reviews.
4. Flexibility and convenience: Both institution and employers of labor can easily verify certificates online.
5. Improved transparency and accountability: The platform maintain transparent records of certificates and reduce fraudulent documents.

## 3.4.1 System Architecture

The system architecture for the Certificate Verification defines the overall structure and components of the system, ensuring that all parts work together to meet the specified requirements. This architecture is designed to support a scalable, efficient, and user-friendly platform for managing certificates verification interactions, shown in Figure 3.4.

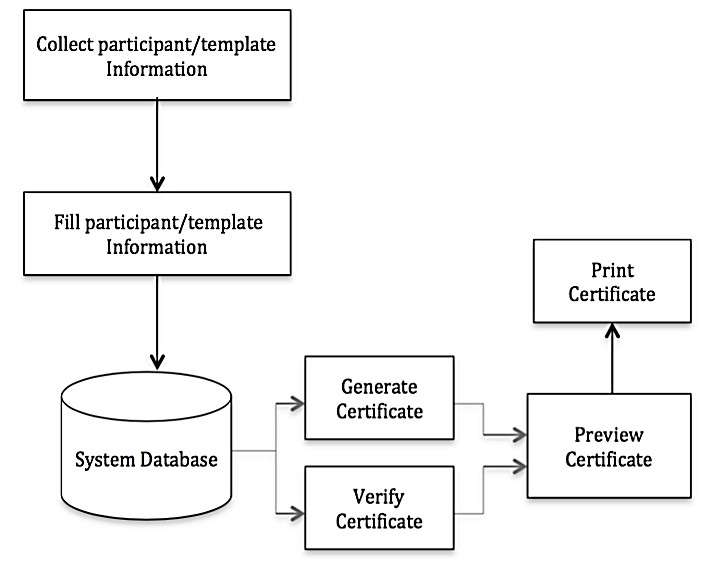


Figure 3.1: System Architecture

## 3.5 System Design

System design for the Certificate Verification System involves defining the platform's architecture, modules, interfaces, and data structures to meet specified requirements. It entails the application of systems theory to product development, ensuring the alignment of design elements with the objectives and needs of the system.

## 3.5.1 Use case diagram

A use case diagram at its simplest is a representation of a user’s interaction with the system and depicting the specifications of a use case. A use case diagram shows the system and the various ways that they interact with the system, shown in Figure 3.2.

Login

Generate Certificate

Add Student

Generate QR code

Admin

Scan QR code

View Certificate

Print Certificate

Print report

Verifier

Figure 3.2: Use case diagram

## 3.5.2 Activity Diagram

An activity diagram shows a flow of control in a system similar to a flowchart or a data flow diagram, shown in Figure 3.3.

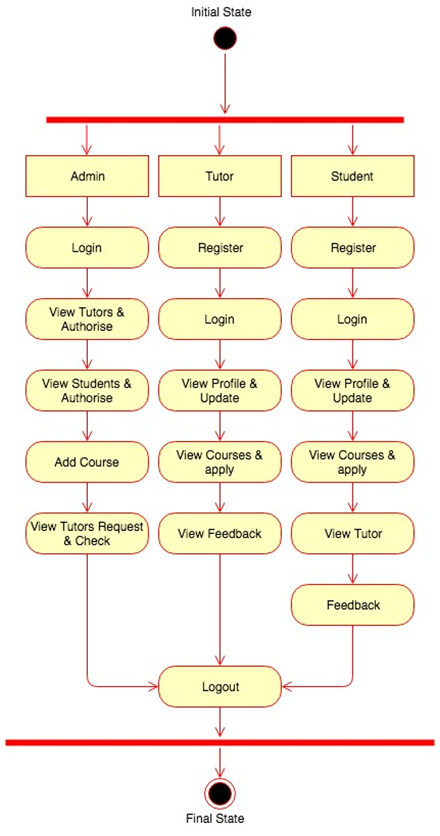


Figure 3.3: Activity Diagram for the system

## 3.5.3 Database Tables/Queries Structures

The database is used to store all information that pertains to the Certificate Verification records. Below are the database tables for the new system.

**Table 1: Admin**

The Admin Table stores information related to system administrators who manage the tutor-finding system. Each record represents an individual admin with a unique identifier (id), a username for login (username), and a password for authentication (password). The id field is an auto-incrementing integer that uniquely identifies each admin, while the username and password fields are used to grant and verify access to the system as shown in Table 1.

**Table 1**

**Top of Form**

| **Name** | **Type** | **Extra** |
| --- | --- | --- |
| **id Primary** | int(11 | AUTO\_INCREMENT |
| **Name** | varchar(50) |  |
| **Department** | varchar(255) |  |
| **EmailId Index** | varchar(50) |  |
| **MobNo** | bigint(11) |  |
| **Password** | varchar(50) |  |

**Table 2:** **Certificate Records**

The Certificate RecordsTable contains details about the certificates available on the institution database. Each record includes a unique identifier (id), full name (Fullname), the course of study (Course), their gender (Gender), date of birth (Date of birth), email address (Email), Quick response code (QRcode), and registration number (regnum). This table helps in managing and retrieving information about certificates for scheduling and inquiry purposes as shown in Table 2.

**Table 2**

**Top of Form**

**Top of Form**

| **Name** | **Type** | **Extra** |
| --- | --- | --- |
| id Primary | int(11) | AUTO\_INCREMENT |
| Student\_id | varchar(250) |  |
| qrcode | varchar(250) |  |
| Date | Timestap() |  |

**Table 3: Students**

The Student/Inquiry Table tracks inquiries submitted by students regarding tutoring services. Each record has a unique identifier (id), and includes foreign keys linking to the relevant tutor (tutor\_id) and course (course\_id). Additional fields capture the student's full name (fullname), email address (email), contact information (contact), the content of their message or inquiry (message), the status of the inquiry (status), and the date and time the inquiry was created (date\_created). This table facilitates the management and follow-up of student inquiries, providing a structured way to handle requests and track their progress as shown in Table 3.

**Table 3**

| **Name** | **Type** | **Extra** |
| --- | --- | --- |
| id Primary | int(11) | AUTO\_INCREMENT |
| Studentid Index | varchar(250) |  |
| Studentname | varchar(250) |  |
| Age | varchar(250) |  |
| Gender | varchar(250) |  |
| Level | Vacrchar(250) |  |
| Department | varchar(255) |  |
| image | varchar(255) |  |

## 3.5.4 Database Entity Relationship Diagram

A Database Entity Relationship Diagram (ERD) is a visual representation of the data structures within a database and the relationships between them. It provides a high-level overview of the database design, illustrating how different entities (such as tables) are interconnected. The ERD helps in understanding the organization of data and the relationships that define how data in one table relates to data in another, as shown in Figure 3.4.

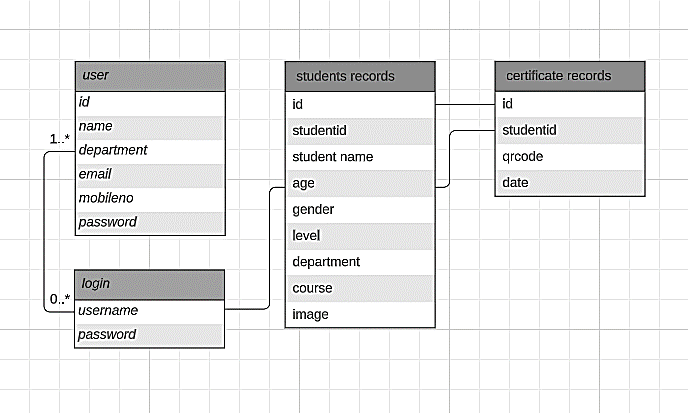


Figure 3.4: Database Entity Relationship Diagram

## 3.6 Software Development

## 3.6.1 Waterfall Model

The development of the Certificate Verification follows the Waterfall Model, which comprises distinct phases as outlined and diagrammatically represented in Figure 3.5:

Collaborating with stakeholders to identify and analyze the requirements for the Certificate Verification, including features, functionalities, and user interface specifications. Creating a detailed system design based on the gathered requirements, encompassing architecture, database structure, user interfaces, and workflow. Developing the Certificate Verification according to the specified design, coding functionalities, integrating components, and structuring the database. Conducting thorough testing of the system to identify and rectify any bugs or issues, ensuring its functionality, reliability, and security. Deploying the Certificate Verification and providing ongoing maintenance and support, monitoring performance, addressing issues, and implementing updates and improvements as needed.



Figure 3.5: Waterfall model

## 3.6.2 Technologies

The proposed system will be designed using HTML, PHP and MySQL as the database management programming languages for keeping records of the tutor finder system. The design also uses the Responsive type of web design where the content of the website fits exactly and the content is not loss when viewed on different device screen sizes and types. Also, the website is compatible when viewed on different browsers from device to device.

**PHP** will manage server-side logic, database interactions, and dynamic content generation.

**MySQL** will serve as the backend database, storing and retrieving all system data securely.

**JavaScript** will enhance the system's interactivity, perform client-side validation, and enable dynamic content updates.

**HTML/CSS** will structure the content, provide a clean and responsive design, and ensure compatibility across devices and browsers.

## 3.7 System Requirements Specification

## 3.7.1 Hardware Requirements

The software to be design needs the following hardware for an effective operation of the newly designed system.

1. A system running on intel, P(R) duo core with higher processor
2. The-Random Access Memory (RAM) should be at least 512MB.
3. At least 20-GB hard disk.
4. A monitor.

## 3.7.2 Software Requirements

The software requirements include:

1. A window 7 or higher version of operating system.
2. XAMP or WAMP for Database
3. PHP
4. MySQL
5. Browser

## 3.7.3 Personnel Requirements

Any computer literate who has a technical knowhow of internet surfing can use the system because it is user friendly.